>> Please be sure to get headsets as we will be having a French speaker.

>> If any of you need headsets, please take them. There is a table at the door and they're passing them out. We will start our program just in a moment. There will be a presenter speaking in French. Thank you.

>> We are going to start in a few minutes. We are waiting for our moderator and we understand he's on his way, so we apologize for the delay.

Thank you, everyone, for the wait. We are going to get started now, and I would like to remind you to please get a translation headset, as we will have a French speaking panelist. And thank you for coming, and I would like to introduce Nii Quaynor, who will be our moderator for today's forum on DNS abuse.

We will have time for questions between panels, and if you have questions, please make sure to identify your name for the translation and for the scribes. Thank you very much.

NII QUAYNOR: Thank you, and welcome. As I understand it, what we thought would be just getting simple names to remember in doing our Internet work is becoming more and more challenging over time, in that others begin to find ways to not use it the right way.

In so doing, it's beginning to create a number of challenges or abuses, and so it's important for us to take a moment and at least reflect, especially in a developing environment like what we have, just in case that there are peculiar observations or challenges that we are discovering that may, indeed, enrich our knowledge globally regarding abuses of the DNS system.

So to help us begin our discussions, we have assembled a very, you know, good panel, very diverse, and we will do our work in two sessions.

There is a first session that will attempt to take a look at latest developments in the fight against DNS abuse, and then we will come back later and have a session addressing the issues of the evolution of the domain name take-downs, which may be a plausible action in response to some of the abuses that we come by.

So what we'll do is, as usual, give our panelists a chance to make their initial comments, and then it will get to the turn of the rest of us to also chip in, and in some cases we'll get the panelists to respond just to make it a little bit more interactive and interesting.

So for the first session, which is latest developments in the fight against DNS abuse, we have a panel comprised of Lanre Ajayi, Frederick Gaudreau -- did I get it right? -- and Gary Kibby and Pierre Dandjinou, who is occupied but I'm sure is on his way here.

So to get us started, we'll ask Lanre Ajayi to begin.

And for -- if you want additional details on any of the presenters in terms of bio or additional information on their background, I believe it's available on their Web sites, so I won't belabor that point.

So Lanre, you have the floor. Thank you.

LANRE AJAYI: Good afternoon, everyone. My comment is going to be in the form of a case study. It is a Nigerian case study.

I'm going to share with you the cyber security challenges we have in Nigeria and how we are trying to manage them.

In doing that, I'm going to show you a list, which I'm sure is displayed on the screen now, of the common cyber security challenges that we all know about. I mean, this is not peculiar to Nigeria but these are some of the challenges that we have on the Internet.

Phishing, spam, scam mails -- which is a variant of spam -- identity theft, denial of service attacks, hacking, cyber-terrorism, and viruses, malwares.

Nigeria is -- there's this perception that Nigeria is the cybercrime headquarters of the world. Please note the world perception, that may not be completely true, but I guess that's the perception around the world.

I'd like to say that some of the challenges we see here, we are actually guilty of them. I'll be the first to admit that we are guilty of some of them, but certainly not all of them.

For example, spam. Yes, I plead guilty on behalf of Nigeria that we do send spam.

And I also plead guilty that we send some scam mails.

I plead guilty that there are phishing activities going on in Nigeria.

Identity theft. We actually do this phishing because we want to steal some identity. I plead guilty.

But I will not accept and I plead not guilty to denial of services. We don't do that.

We don't hack, because even if we want to do that, we don't have the technology to do it.

We are not into cyber-terrorism, so I will plead not guilty to that.

And we don't even send viruses because we don't simply know how to write the codes.

And in fact, we are victims of viruses. We receive tons of it from you guys.

So I'd like to plead guilty to the first four, but certainly not to the last four.

And just for doing those four things, we get seriously penalized. You people over there have stopped doing businesses with us on the Internet. That's a very severe penalty. In some cases, you have blocked Nigerian IPs. We can't even access some of your sites. You won't accept our credit cards in some cases.

And we also discovered that when we meet in events like this and we want to chat with you, try to make friends with you, the topic of discussion is usually about a scam list, which we call 419, and we actually find that embarrassing.

So these are some of the consequences of some of our (indiscernible) on the Internet.

And it got to its peak. Sometimes -- some few years back, a senior citizen of one of the Eastern European countries fell into the hands of Nigerian (indiscernible) and the man lost his entire savings. He went to the Nigerian ambassador to complain. The ambassador tried their best but they could not track down the scammers.

The man requested to see the ambassador, the Nigerian ambassador in his country. He saw him and shot the ambassador to death.

That was very serious.

So as a country, we had two options, perhaps.

One option is (indiscernible) to declare war against our country for killing our ambassador.

The other option is to allow that country to do the right thing, to allow justice to take its course, and for us to look inward and tackle the menace.

The Nigerian government settled for the latter. We left justice to be done by that country, and we decided to look inward and fight cybercrime in the country.

So how did we do that?

The president set up a national cybercrime working group, of which I was privileged to be a member, to find a solution to this menace, and the group worked very hard and we came up with a number of solutions, a number of attempts to curtail the menace.

One, we looked at the legal angle, we looked at the technical angle, policy angle, and we tried to attack it from various angles.

From the legal perspective, we discovered that our law is very weak on cybercrime. For example, there is no law against spam. If you send spam, if you send even the scam mails and you are caught, there is no law in Nigeria that says you have committed any offense.

So we came up with bills that address some of the issues, and the bill that was drafted by the cybercrime working group thoroughly addressed the issue of spam, it addressed the issue of a lawful intervention, so it is not legal -- when the bill is passed to law, because the bill is still with the Parliament -- when it is passed to law, it will be legal for law enforcement agencies to actually intervene into communication transactions going on.

And electronics evidence was not there. It's still not there until the law is passed, and it's a challenge.

A couple of people who were arrested were not -- we were not able to convict them because the only evidence available for cybercrime usually is electronic evidence, which is not tenable in Nigerian courts.

And we recommended an amendment to our evidence act, which has been accepted.

And we also thought that we believed that the industry also has as a role to play. I mean, the operators who are making money providing services. So we encouraged them or make it mandatory for them to come up with a voluntary course of conduct which will be mandatory for their members, and the erring members will be blacklisted.

And we also realized the importance of education in all of this.

We discovered that these scammers, they carry this impact of people around them, because the people do not appreciate the implication of the activities on our national economy.

The argument has always been that it takes two to tango, that it takes a criminal out there to collide with a criminal in Nigeria to do all of this, but on the other hand, we think it's not good for our national image, it's not good for our economy, and we should also let the general public to know about this, so we emphasized on education, on public education, public awareness on all of this.

And now, importantly, as this discussion is related to domain names, we noticed that most of this crime, most of the listed cybercrime I mentioned earlier, cannot be done without using the domain name in one form or the other.

In most cases, these criminals will clone the Nigerian government Web sites, and it was so easy to do that because in Nigeria, most of the ministries, departments and agencies in Nigeria, they do use the Nigerian top-level domain name. They use the generic top-level domain name, .com, which was strange, so it was very convenient for the criminals to take a .com that looks very similar to government agencies' Web sites and clone it, to make -- to commit all sorts of crime.

So we also recommend -- we recommended to government that the use of a .gov.ng is mandatory, and I think that one has been followed now.

With all these steps taken, I'm glad to report to you that cybercrime is actually going down in Nigeria.

And now I am pleading to you to please do business with us. Stop blocking our IP.

Thank you very much.

[Applause]

NII QUAYNOR: Thank you very much.

Actually, as I recall it, the name 419 itself --

LANRE AJAYI: 419, yeah.

NII QUAYNOR: -- was itself an action against identity theft.

LANRE AJAYI: Correct.

NII QUAYNOR: So you must have been in the history for a long time to solve this problem.

LANRE AJAYI: Correct. Thank you very much.

NII QUAYNOR: Okay. So with that, I'd like to get a slightly different perspective so I'd like to invite Pierre Dandjinou, if you're --

PIERRE DANDJINOU: Thank you very much, and sorry for being late.

Well, I'm from Benin and I really like what my colleague has just said, that this thing is going down in his place, because we are neighbors and we are always, you know, fearing what's happening there in Nigeria, what is going to maybe having any impact on us in Benin or Togo and the rest of the places.

But of course mine is going to be quite a sort of brief reporting on what has been -- what we've been doing in Africa to actually combat, you know, this phenomena.

We really see that in Africa, at least, decision-makers are really getting interested in this issue.

They have come to notice that of course while the Internet is pervasive, DNS abuse is something quite important. They are more and more keen on actually giving some resources there so that the appropriate -- so the appropriate, you know, mission will be conducted, which is quite a good thing.

Now, we would have loved to have, you know, some of the statistics, you know, through some sort of screening ccTLDs in operation in Africa, and unfortunately those data are not that much available.

As Lanre just said, there are issues anyway. We all know there are some forms of attack, you know, in the different places, and sometimes it's always due to kind of poor infrastructure that we may have in different places, sometimes the inability to properly run some of the servers we do have, and also the whole issue surrounding DNS, DNSSEC I think we -- really needs serious consideration from Africa, both from the professional perspective and also from the policymaker's perspective.

Now, given all of these, you know, sort of environments we do have, so what is being done or what has been achieved?

I will say we do have different approaches here.

We have the professionals, actually, who, through some of the network, you know, (indiscernible) training that we do conduct, you know, under an invitation by AfriNOG, which is (indiscernible) and now we have started to do some workshops, specific workshops on cybersecurity, and that's helped us now actually build more and more capacity, have more and more people that are actually trying to get certifications so that they are able to fight and at least to make sure that there's an instant response to whatever disaster management strategy, you know, in the countries.

One of the efforts on the ground is the Africa cert. Africa cert is coming as kind of a regional initiative that really wants to build capacity in different countries, because as you know, although we speak of Africa as 54 countries, there are different situations, there are different conditions.

We heard from Nigeria. We'll have another story from South Africa, or even from Togo.

So an Africa cert is kind of a continental initiative that really wants to do a few things.

Of course one of them is sensitizing decision-makers that this is a reality, because in most places, as long as it doesn't come to security issues, they don't really understand. So one of the things we want to do there is sensitize decision-makers, have a full sort of fledged program for policymakers. We have started, you know, some of the classes for policymakers on cybersecurity. But also, we want to train more and more people that could provide responses.

Actually, right now, we don't -- I think we have something like close to five, you know, countries that have really worked out their cert, you know, national cert.

The idea is to have more and more of them.

So Africa cert is going to work closely with, you know, national professionals to make sure that they do have their own cert.

Africa cert is also -- would like also to be the repository, what I will call the -- yeah, the repository of whatever documentation you need, information you need, statistics you need, to combat this.

And of course Africa is also not going to (indiscernible) thoroughly, is going to be working through cooperation or partnership with the industry, but also with other, you know, players.

We know that ITU has its own impact program, and certainly we will not be -- we will be certainly working together with those.

We'll intensify the workshops, you know, on DNS abuse, and we have planned for that, and Africa cert is -- itself. We are actually trying to register this and then so it has full operation, certainly 2012.

And the other thing that is happening in Africa is the program for, you know, law enforcement, and that one is AfriNIC, the African Internet registry, has established this program, and this is three or four years ago, and wish typical targets -- you know, lawyers and government, you know, officials -- to actually not only sensitize them but also introduce them to the needs, you know, for revisiting the appropriate legislation in different countries.

So this is a well-attended meeting as well, this law enforcement workshop that AfriNIC had.

So which means that like I said, governments positions are more and more, in fact, interested. In fact, some of the -- that's a big story. Some of the -- in a recent sort of -- yes, thank you very much -- election, in some of the places in Africa, we have something quite specific kind of (indiscernible) phishing, where some of the content (indiscernible) will be having their Web site directed to the opponent's one and there was no one to provide any answer to that. You go to the election committee, they say, "Well, that's the first time we hear this thing, we don't know what to do about it."

So you will have some of those stories happening in Africa, and you need to educate people on those.

And the last thing is what has been done by INTERPOL. INTERPOL is kind of quite active, and working with kind of police and admin departments and basically for capacity development in some of those police guys. Also we had a workshop, kind of interesting one, because of the specificity for them to actually conduct those missions.

We'll have places where there was some sort of partnership between the police and the (indiscernible) guys. I think Cote d'Ivoire is one of the places where there's a kind of symbiosis between the police and the -- and there are a few places there is still some sort of lack of trust, you know, because it's about national security, so it's difficult for them to include, you know, professionals, so we need to actually talk to them, we need to make sure that they do understand the technologies that exist there, and then they can use it.

So, yeah, this is some of the things that are actually happening in Africa today. Which means that, yes, we are trying to make sure that these things move smoothly and I will say this is good news, anyway, that things are happening in Africa. Thanks.

NII QUAYNOR: Okay. Thank you, Pierre. So we've seen a national case and now we've seen some of the activities at a regional level, and I'm really very pleased to see that AfriNIC and AfriNOG continue to support the cert activities that you've initiated.

Anyway, let's move on. It will be very useful to now get out of the continent and learn maybe a different perspective, some words of encouragement for us.

So I would like to, you know, invite Frederick Gaudreau, of Surete du Quebec, Canada, to share a few words.

FREDERICK GAUDREAU: So for those who will need translation, because I'm going to speak in French...

(Scribes not receiving English translation.)

That's why we see that in reality -- in African reality that we are nowadays, there is an increase in the numbers of Internet users. And we will -- the capacity of Internet access with better bandwidth in the African community, there should be an increase of cybercrimes. That's inevitable. And it is going to be a tsunami. So the needs in terms of training for tools is very crucial, and that's why international cooperation is crucial.

So we take this opportunity of this forum at ICANN to regroup 30 police officers, law experts and judges to assist a workshop on cybercrime and to listen to their needs in or to provide more substantial assistance with regards to their knowledge and training. ICANN made it able for us to hold this forum and this workshop. And the judges and police officers were very happy for this training.

So that was the objective, the aim of this presentation. So I hope you can see the initiatives that are being launched, and this is in addition to what my colleagues said here. And I'm willing to answer any questions you would have. Thank you very much.

NII QUAYNOR: I think it is good we have some initiatives, and it is also good comments to share with you that Cote d'Ivoire is addressing issues. (Indiscernible audio)

Now we come to Europe. And we are very fortunate to have Gary Kibby, Serious Organised Crime Agency, United Kingdom, to share with you.

Please.

GARY KIBBY: Thank you very much. What it reminded me from the outset is that I must speak slowly for the translators, and I will speak as slow as possible and as clear as possible.

I actually wanted to touch on two particular areas. One is actually to talk about the work that my agency and other law enforcement are doing in relation to DNS abuse; and then really the second area is a bit of an operational conundrum that's there, that I'm actually looking for the community to actually give some thought to about process, where we find ourselves in investigations with particular problems. And I just see this as an opportunity to share with you a particular problem area.

First of all, SOCA, Serious Organised Crime Agency, is a U.K.-based agency. It is a combination of police and other bodies brought together. We have a slightly different remit from traditional law enforcement because we look at problems, problems with criminality. And I'm in the cyber department, so one of the areas we are looking at is DNS abuse because -- obviously from the organized crime perspective down to normal crime. Somebody asked me what is "serious crime" as opposed to "ordinary crime."

But really the DNS abuse touches everything. So everything we have done over the last few years has been based on real, live operational cases. This isn't a dream factory of people entering into the area. That's why we've engaged the community. We've been along now to probably six, seven, eight, nine different ICANNs in terms of law enforcement representation.

We're now working with partners in law enforcement across the world. We've done some work. Already mentioned early on in relation to the work that's gone on within AfriNIC, we are working through the RIRs to actually work collaboratively with the law enforcement in the regions across the world.

We've had at various ICANN meetings representatives from South America, representatives from Africa, representatives from Asia. And certainly the European presence has always been constant. So this collaborative work in terms of working with the ICANN community is really important to us.

And now obviously Mick has been representing INTERPOL, is now an observer within the GAC to bring forward the law enforcement views. So in terms of what have we been doing around DNS abuse, I won't go into any depth because I'm conscious of the time.

Obviously, the hot topic at the moment -- and I won't go into any detail -- is obviously the law enforcement RAA amendment around, you know, what we would see is dealing with a number of areas where there is greater due diligence required.

We're contributing actively. We've got a senior law enforcement officer actually from my agency, my boss, Sharon Lemon, is actually an active part of the WHOIS review group, which is another first for law enforcement to be involved in review of a process. As I've said, we've got the working groups.

I think from law enforcement, the DNS abuse area, what we are concerned about is to identify the things coming over the hill, the things that will impact on our work and investigations. And it is the community and yourselves who will identify areas that are going to be real problem issues for us. At the moment, such issues as IPv6, gTLDs, the new gTLDs, IDNs. We've even had two offices from FBI and RCMP attend the first IETF, are really getting into understanding the development of the Internet for the future. So these are important areas.

And because for law enforcement, this is a global challenge in terms of within the ICANN community undoubtedly, we are a minority group. Unfortunately, within law enforcement across traditional business, we are also a minority group. There is a lot of law enforcement. You do not understand the importance of the work that is going on within ICANN. And our representation as law enforcement here, we then need to feed back to raise standards across all levels of policing.

So the one particular area that we find ourselves dealing with at the moment is a particular problem around the distribution of malware. We all know what malware is. We all know that criminals will take every opportunity to exploit weaknesses in systems and processes because that's what criminals do. They're there to make money.

So we're not going to get into the technical aspects because I do not understand them. At the end of the day, that is way beyond myself. But we are talking about domains where they're using the command and control in terms of they only need to take this domain name -- and this is my only slide in terms of what is being registered. And this is being continually registered throughout the registrars. There is no indication that there is collusion in this. But these domains will be used for the command and control. And the command and control will actually only need to be in place for a matter of hours for them to carry out a malicious attack.

Now, you would look at those if you were an English speaker and say, Well, what do they actually refer to? Well, actually they refer to nothing. They are just automated algorithms that are there that are churning for these criminals. They just churn these all the time. And what they're doing is finding weaknesses in our systems and processes. And I use the word "our" because I wish to be inclusory. But the processes that are currently in place for the identification of criminal activity do not address this problem because obviously once they're identified, you have a process to go to the registrar in terms of contacting the registrant. If it is clearly criminal, maybe 15 days. These people need less than 15 hours.

So we don't have a solution. But what I'm doing is sharing a particular operational problem in terms of process.

We would say as law enforcement, greater due diligence at the outset, looking at the registry. Why would they want to register such names? Do they have any sort of commercial value? So each of these is actually supported by bad WHOIS.

The WHOIS is actually improving in criminal terms. Before it would be empty, or it would be Mickey Mouse or something. Now it requires a reasonable amount of due diligence to drill down into actually this is bad. So they are getting better. They are learning because the more that we do from law enforcement and industry and many people on this stage here who are assessed, the more they learn, the more they respond. And certainly in terms of -- the WHOIS issue is an important issue for law enforcement.

Again, the money is an issue around these registrations. Again, they will pay with stolen credit cards. They will pay with virtual money. These are all opportunities.

And, really, I'm just sharing this with the community because if anybody has got any ideas, that's the area. It's process, weakness, in terms of -- really, that's the two areas that I wanted to cover. So thank you for the opportunity to share these two areas.

NII QUAYNOR: Thank you very much. Let's give him a hand.

[Applause]

These have been very good. I have heard very important words. I have heard "collaboration." I have heard "education." I have heard that we have to build our communities. And now I'm hearing that there are some process challenges.

Anyway, I think it is now your turn. I would like to open it up for some questions and some comments. And you would have a chance to react at this time. So, please, open mic. We have ten minutes or so to work with.

STEVE DelBIANCO: Thank you, Steve DelBianco with NetChoice. Gary, question for you. Can you elaborate a little bit on the specific RAA amendments that you were working on and whether you think they will actually be effective?

GARY KIBBY: I think the issue of the RAA amendments; I don't think that -- I think they're well documented in terms of the law enforcement recommendations. They've been put forward. And I was in with the discussion yesterday between the GNSO and the GAC. I think these recommendations go some way to addressing some of the issues around DNS abuse.

I think the criminals are part of the evolutionary process. And we've all got to learn that whatever process that we follow, the criminals will mirror that. So it is a matter of actually just keeping -- sharing from both sides.

So in terms of the specifics about the recommendations, I think they're well documented. And I don't think there is any value in going over the specific recommendations in this forum.

ANTOINETTE JOHNSON: You may have addressed this during the session, but in the bid to curb --

MARGIE MILAM: Excuse me, your name, please?

ANTOINETTE JOHNSON: My name is Antoinette Johnson.

In the bid to curb DNS abuse, how do you avoid actually not blocking genuine DNS queries? Sometimes in the case of the country I come from, we find that general I.P.s are blocked or restricted because people are trying to curb the DNS abuse.

NII QUAYNOR: Lanre, do you care to comment on that?

LANRE AJAYI: I think in the next session we address the DNS takedown. And maybe we should leave it to the next session for proper discussion of the DNS takedown.

>> My name is Mary. I'm from Nigeria. And I want to say that law enforcement against this are really upbeat on crime/cybercrime security. And some of the findings, one of them is that because of the process in the domain name registration and I.P. (indiscernible), when they trust the I.P., it may not be from AfriNIC. It may not be from Nigeria. It might be from anywhere. It might be from China. It might be the legacy I.P. addresses. So it is very difficult for them to trust and get to the face behind the crime. That's one bit.

The other bit is that it seems to me when the whole issue of computer talking to computer was developed by the Internet, nobody thought of how to put the face behind who has a (indiscernible) domain name or the I.P. address. So I think whoever wants -- however we want to fight this, whether it is from the law enforcement side or where, we need to see the IPv6, will it address that gap that IPv4 didn't have? That is the face behind because you can really start from anywhere. So it may not necessarily be all these problems are coming from Nigeria. That's what our law enforcement has established. But the fact remains that you cannot -- they cannot trust, they cannot lay hand on who registered the I.P. or the domain name that is being used for abuse.

Okay. So I would challenge that we -- the Internet community look at that, how do we get that on board so that even when we are doing the cybercrime or cyber security, abuse, or whatever we want to do in (indiscernible), because just like the last speaker said, blocking the genuine ones because it is banned -- it is taken as a whole block. These are really blocked because of the process of DNS usage and I.P. address usage. Thank you.

(Scribes receiving French translation)

ROD RASMUSSEN: I would like to make a comment on the Nigeria question (inaudible audio). I have to commend -- Nigeria law enforcement has worked very diligently with U.S. law enforcement in particular on addressing the 409 issue over the last several years. I know there have been a lot of joint operations, some very interesting ones involving heavy weaponry.

I think that Nigeria has taken that problem on very seriously. What we see is that now a lot of the people doing that are going across the border in order to commit the same crime. So when you push down on one place, they'll move to another place to commit crimes. Now other countries are involved as well. It is one of those things that, again, exemplifies why it has to be a global solution to the issue.

I didn't really have a question. I just wanted to give you guys -- give the Nigerian officials some real support for the work you've done. Thank you.

NII QUAYNOR: Go ahead.

LANRE AJAYI: I just want to thank him for the compliments. The truth is we are doing a lot to curb the menace. I think the first thing we did was to admit the crime problem existed. It did exist. The cybercrime -- they come from Nigeria. That is the truth. And the government admitted that set up a whole agency to fight crime, ESSC. And they have been collaborating with other agencies from around the world, the U.K. They do some work in Nigeria. The U.S. do some work in Nigeria. We are collaborating, and we are fighting the criminals. And the criminals are leaving Nigeria. Nigeria is almost crime-free now as a result of the good effort of our law enforcement against it. I want to repeat again you are free to transact business with Nigeria.

NII QUAYNOR: Very good. Last comment.

>> (saying name) from Estonia Internet Foundation. I want to have a comment on Gary Kibby's problem which he pointed out last so there is accuracy of the WHOIS. It is very hard for law enforcement to get information who is really behind this domain.

In Estonia, last year we developed the solution where in domain registry with every domain name, there is a connected private person or a company who is responsible for this domain name and this private person or company is also identified. So there are no anonymous registrations in domain registry.

Although we have quite a small number of domain names, it is about 64,000, this solution can be scaled also internationally because it is based on this FATF 40 plus 9 recommendations for anti-money laundering and terrorist financing.

And according to this (indiscernible) group of financial (indiscernible) units, this framework is already implemented in more than 100 countries. So it basically works that we track money online. We have also modified this EPP protocol so a registrar can attach to this EPP query, information improving this authentication of registrant. With a domain name registration, we live store this authentication data to our center of registry. Thank you.

NII QUAYNOR: Thank you very much.

GARY KIBBY: In relation to that, I would just like to thank you. That sounds most interesting, and certainly we will take that up offline.

NII QUAYNOR: All right. So thanks very much for your participation in the first half. We'll move onto the second half right away. And this one, this is in recent times, domain takedown processes for dealing with cybercrime and other malicious conduct involving domain names have evolved from theory to practice.

In the absence of uniform ICANN policies to address these concerns, security professionals, law enforcement agencies and private companies rely on voluntary cooperation or legal process to accomplish these takedowns. The panelists will explore the effectiveness and challenges associated with these practices and what role, if any, should ICANN play in the evolution or the domain name takedown practices.

To help us at least bring up the issues quite clearly, we have a number of -- I think it is four -- we have four presenters. And so I'll just ask Michael Moran from INTERPOL to lead the discussion.

MICHAEL MORAN: I would like to start in French and see everybody panicking and looking for the headsets. And then I'm going to continue in French.

I will continue in English. I'm an Irish police officer as you probably already figured out from my accent. And I want to comment to INTERPOL.

And, you know, this whole area of what can ICANN do about domain names and what can anyone do about domain names got me thinking about what perhaps domain sellers and registrars and everyone else could do about domain names. I thought it might be a nice one just to open on the idea of Mr. Public Joe, otherwise known as Joe Public. His mother calls him Joseph, of course, but everyone else calls him Joe.

So Joe Public goes on to find out and somebody has told him that he can go to a WHOIS database and he can find out where the domain comes from and the person responsible for it. So he does that. Eventually he finds himself going to Network Solutions' Web site, for example, because they are listed as the company who sold this domain. So he goes there, as I did, even up to an hour ago. And he attempts to find where on this Web site he can go to report that he has a problem with a product that was sold by this company.

So he goes there, and he goes through all of this here. Now, he can buy all the domain names he wants. He can get 40% off SSL certificates. He can even go down here and get 40% off -- oh, he can go and by a XXX domain because sunrise is here. He can go and get his mobile Web site. He can go to get a Microsoft-hosted exchange. He can even go down here to the small print, and he can search and search and search and he won't find abuse anywhere. He'll try.

So he'll -- perhaps he will try and contact the company. So he will go to the contact company and in here, he will find all he needs to know about sales and support, if you are already a customer. However, he won't necessarily be able to find anything about anything. Right? He can't find it anywhere.

So, he decides he'll do another little bit of looking. And he rings his brother Peter. And Peter Public decides he will go and deal with the person he had a problem with, the domain he had a problem with last week. And he find himself on the ENOM Web site. So.

He goes to ENOM because they are the ones who sold this service to the person who has created the problem for Peter Public. So he goes to the ENOM Web site, and again he goes through all this. But in fairness to ENOM, when he goes down to the bottom and he gets by all the nice young-looking ladies and really shiny, happy people selling ENOM API plug-ins and other things, he goes to the bottom and eventually actually in fairness to ENOM, he goes to the bottom and he finds "report domain abuse."

[Applause]

Well done, ENOM. Fair play. So he goes in and he says, "I want to report the fact that I have been malwared by one of your clients." So in he goes, and he finds actually that he can't report anything to do with child pornography, malware, phishing. But he can report spam. He's received some spam. So he can report spam. But at least he can report, because when he rang his cousin Phileas, Phileas Public, he had a problem with Go Daddy, who are a wonderful, wonderful company, Go Daddy. Again, lots of shiny happy people selling lots of shiny happy products, as is their business -- and I will never criticize a company for making money, because that's what companies do, isn't that right?

So he goes along and he gets past all the shiny happy people, and the fact that it's only $9.95 for new dot coms this week, and he gets down and he goes along all the lines on top here. He can't find any problem here. No, can't report anywhere. Hmm. Oh, look! "Report spam"! But it's a malware problem I want to report.

But it's okay. At least he can report.

So he goes to report spam and he goes in and he finds that he can put in his name, his address, his e-mail address, and then he's got a drop-down menu!

So is it possible he can report the phishing? Is it?

He can report spam news group, spam weblog, spam guest book, spam forum, spam pop-up, spam WSM, spam IM, spam chatroom, spam --

Look, at the very bottom! He can support -- he can report miscellaneous!

So well done, Go Daddy!

[Applause]

Except that it said "spam" on the front.

But I can also report phishing. That's true. But I can't report child abuse material. I can't report anything else.

Well, I can, of course, because the facility is there.

But perhaps what I'm trying to get across here -- and very quickly, indeed, in the time that I have left -- is that why is it that some companies won't take any report at all, it's actually quite hard to find them, and some companies will only take a report of spam or show that they will only take a report of spam.

Now, of course I can report anything because I'm Phileas Public, Peter Public, and Joe Public, and I know, I'm a reasonably intelligent human being and I know I can report this material without difficulty, even though -- I can report it as child abuse material even though it says I can only report spam.

And I have to ask: Why is that? Why is it only spam? Why can't abuse be reported in a normal way?

Why... can't... spam... be... re- -- I'm sorry. I'll slow down.

Why can't spam be reported in a normal way, or why can't any other crime type be reported in the same way spam can be reported by the two good actors who will take a report, rather than unlike the first one that we looked at who won't take any report. He's not interested. Is it a question of interest or is it just getting away from the spirit of RFC2142, which sets out -- written by a guy called Steve Crocker. I don't know, he's probably an old man now enjoying his dotage in a meadow --

>> That's actually Dave Crocker, his brother.

MICHAEL MORAN: All right. Really? Okay. Well, I know there's Steve up there now. Steve is in there somewhere as well. Steve added on some stuff to it, so Steve and Dave are probably two old men now smoking their pipes sitting on a veranda somewhere enjoying the sun going down.

But in it, if we search we find the word "abuse" and we find that there's a number of issues, one of which is that, you know, domains should have abuse at domain dot whatever. They should have that for customer relations. For what? For inappropriate public behavior.

Now, I accept that companies will have to put resources into this, and I accept -- I expect that there would be a huge amount of -- a huge amount of -- I expect that -- thank you. Anything else? What am I having for tea tonight? Maybe you'll let me know? What am I eating for my dinner?

>> Your time is getting finished.

MICHAEL MORAN: Why is it? Because, you see, the three companies that I showed you there are three of the biggest companies, and they're breaching the spirit of this RFC.

And not only are they breaching the spirit of this RFC, but they're giving a terrible bad example down to lower actors within the field.

So you have the top and then you have lower resellers and domain sellers and all the way right down to some of the smaller actors in this game. And the bad example starts at the very, very top.

And not only that, but it just creates a perception that if you have a problem on the Internet, well, tough. You know, it's your own problem.

Because it certainly isn't mine. And I would like to see that changing. Thank you very much.

[Applause]

NII QUAYNOR: Thank you very much. That was very clearly stated.

[Laughter]

NII QUAYNOR: Next I would like to invite Rod Rasmussen, Anti-Phishing Working Group from the U.S. to share a viewpoint.

DON BLUMENTHAL: I'm glad you're next.

ROD RASMUSSEN: Yeah. Tough act to follow, right?

DON BLUMENTHAL: Right.

ROD RASMUSSEN: All right. Hey, this thing works. Excellent.

So I'm actually going to -- now, in following in the spirit of Monty Python that we brought out earlier, "And now for something completely different!"

So I'm going to be talking about the -- something that many of you have heard about before, but we're actually ready to go with, and this is the abuse of domain name resolution suspension process, or ADNRSP. We in the APWG like acronyms just about as much as ICANN does.

So for those of you who haven't heard about this, or just to review, the idea here is that you have a trusted way for people who are law enforcement or people who deal with domain name suspensions on a regular basis, whether it be a large brand bank or companies and security professionals who do this all the time, to have a trusted way for registries to interact with them in a very precise and controlled and audited fashion.

So create a trusted system for doing domain suspensions.

And this is really to get -- get to the heart of the issues we've had over the years where everything is ad hoc and there are not really good hard set rules for how people interact when you're trying to do a domain suspension and build more trust in the system and build scalability and, in theory, better speed into the system so that you're dealing with trusted parties at scale and you can do this in a repeatable process that's auditable.

So this is really trying to make the -- this whole industry mature a bit.

And this is strictly for domains registered by criminals. It's not for suspending domain names that are simply compromised. And in the case of phishing, that -- actually, most phishing sites are on compromised services. Either the domain name has been hacked in -- or the server has been hacked into or there's some sort of shared hosting system or the like. It is not a domain name that is eligible for suspension here. This is simply for the domain names that are registered and held by the bad guys, so to speak.

And there's a whole series of indicators for what those are and I'm not going to delve into the details here. They're the normal things you would think of, and they're -- also part of the process of reporting the domain for suspension is filling out the criteria here.

And I already discussed the ad hoc way that we're doing it today.

It adds a lot of risk to both the intervenor, the people trying to get domain names suspended, and for the party on the other side of the equation, either the registry or registrar that you're dealing with.

And that is a -- has been a problem all along and it has caused, you know, certainly lots of consternation for everybody. So we're -- that's really the driver behind doing this.

The key here is that we really want to get these systems replaced and build a model where we can expand handling of abuse to a wide range of a trusted community and get faster than our opponents at dealing with these issues.

Right now, we have a speed and kind of -- we have barriers amongst each other. Even though ostensibly on the same side dealing with these things, we have barriers that the bad guys don't, and we want to overcome those.

Here's some -- we're in beta 3.1, so we've been at this a while. Some of you may remember my first presentation I think on this was in the Los Angeles ICANN meeting, to date it. That was when it was merely an idea. We now have this -- as you can see from the screen shots here, we have an actual system. We're looking to -- the APWG is having a meeting next month in San Diego where we're looking to launch the actual beta program, and this is a beta program where we'll actually be doing live suspensions so it's a really working beta program.

So we're working with our own beta group within that. I'll talk -- I think a slide on that in a few minutes but if I don't, I'll just give you some more details there.

The -- as I mentioned before, we have explicit criteria and people are aware of that. It's all documented.

There's a ton of documentation for people to fill out to enter the program, to make sure that we have a legitimate party, that their employees are verified, and that their corporate and financial and insurance are all covered, right?

So we know that the person who is making a request, if they have a problem with that request, there's a way of making sure that you have some sort of recourse.

This is what an applicant sees. There's a whole process to go through an application to become a user of the system, and there are various roles that are played. An enrollment manager, and then there's a committee within the APWG that actually goes and checks out the credentials of whoever is applying to be in the program, made up of experts in the field, to vet that organization, and then there's subsequent checks for any individuals who are added to the system underneath that organization.

This is what it looks like to the intervenor themselves. Again, real working software. I've gotten the bug reports over the last year or so, and it's pretty much ready to go.

Let's see what else I've got here.

Here is the minimum -- here's what a request looks like. You have to enter a domain and a full URL of whatever the Web site may be, if there's a Web site involved, and you have to have two prior, I mean, very high requirements. Obviously there's malicious content and there's no legitimate content. Pretty straightforward. But you have to attest to that.

And you sign it in blood. Well, electronically you sign it.

The -- then you have -- well, here's a look at what the attestation looks like, and you actually have to -- you know, "Here's the deal" and I have to put out the various criteria, and so -- and then say that you've done that.

Now, what this allows for is tracking of lots of statistics around what is being -- what is being suspended or what is being requested to be suspended. So it can actually drive some of the further research and further things that we want to do as a community to address these issues.

So we're not only doing this from an audit perspective, but from a research perspective as well.

Here's what a registry would be able to take a look at. They get a request in, then they can decide what their process is for dealing with the particular request. That will often be pushing it off to a registrar in order for them to take care of the problem, because they have the actual business relationship with the registrant.

But the -- this is focused on the registry level, again, for scalability. And you can reject, accept, or request more information, so there's a back-and-forth process.

Oh, I'm getting an invitation for tea, too.

It's in one minute, so I better wrap this up.

Now the clicker isn't working. Here we go.

And there's a tracking system here, too, so both sides of what's going on can get information and see what the status is of various requests. So -- oh, hey, this is the last slide. Hey, that's good timing, huh?

All right. So in summary, we've created a system, as you can see, that's rigorous, rootenizable -- however you pronounce that -- scalable and auditable, and we're adding more beta program members. We have seven registries -- about half cc, half gTLD -- that are at least interested in the program or participating directly in the program, for the most part.

A couple of those are not -- have not made that information public, so I don't want to name names here, but there is at least a couple that are fairly sizeable.

And I know that I've talked to many different registries over the past couple years that also are not on this list yet but have expressed interest.

So if you are a registry and even a registrar -- we want to expand this program eventually -- please contact me or Peter Cassidy. Thank you.

NII QUAYNOR: Thank you, Rod.

[Applause]

NII QUAYNOR: Okay. We move on to Don Blumenthal from Public Interest Registry U.S.

DON BLUMENTHAL: Appreciate it. I don't have any slides. Miracle.

ROD RASMUSSEN: There you go. I'll get your name up.

DON BLUMENTHAL: My students usually freak when I don't come in with slides.

I'm here for the Public Interest Registry, and obviously our service role in domain takedowns, which is in the title here, is that we get law enforcement orders saying to take the domain out of the system.

PIR has -- is and always has been interested in working with law enforcement, in helping out. I think it's part of the name of the organization, the "Public Interest Registry," and it's always taken that public interest role very, very seriously.

Now they've got an ex-Internet law enforcement person on staff, so they've got the extra conscience of doing the right thing.

I was in -- in law enforcement for the Federal Trade Commission for many years.

But I think when discussing these issues, it's important to step back and try to define terms. We hear "server takedown," we hear "domain suspension," we hear "redirection," "domain blocking," "domain filtering," and a number of other terms that are used in Internet law enforcement.

And I think part of the role that we can play, or at least that I can play right here, is to suggest that all of those different techniques have different strengths and weaknesses. You know, the critical thing in any Internet law enforcement action is to get the content out of the system, to make sure that it's unavailable. And there are times that "takedown," as it's commonly termed, or "redirection" is just flat out not the best way to do that.

You know, in an ideal world, we could do what we did in the early days of the FTC. We could go to a judge and say, "Order that server shut down." Well, that was easy when the server was in Virginia and the judge was in Virginia and we were in Washington, D.C. You know, we all -- we all did this within a 15-mile radius.

Obviously that's not possible anymore very much, if at all. People have become too clever in terms of dispersing content using different domains, different top-level domains, and other techniques to try to avoid these types of actions.

But again, each measure has its strengths and weaknesses and each measure has potential ancillary effects where sometimes you've got to look and ask, is the remedy -- are these side effects worse than the remedy?

There is -- right now, there's a current debate in the U.S. concerning the use of redirection. Redirecting traffic can be very useful in certain situations, but in others, it may not be. Specifically, say, in intellectual property issues where people are going to have an incentive to try to avoid -- to evade the court order. It's simple to do it. So the question has to be asked, "Is this really worthwhile?"

On the other hand, redirection to stop a spammer, to stop malware -- well, I don't know a whole lot of folks who are going to try to go get spam or malware, except other criminals who want examples. I don't know.

But it's a constant balancing act, I think, to really try to mesh what the objective is with the proper law enforcement mechanism that is put into place.

I think the other piece there -- and we were talking about this in some sessions recently -- is for law enforcement and the registrar/registry community to be in touch with each other. You know, we can help with using the right terminology to accomplish what's necessary. We had a takedown order not long ago where it said -- where it only gave us half the information necessary to get it done. We wanted to do it, we wanted to do it now, but we had to go back to the U.S. -- to -- we had to go back to the prosecutors and say, "Got to rewrite this, folks, because we can't do it until then."

I think there's a place to work with law enforcement to try to tailor the scope. About a year or so ago, there was an incident in the U.S. where there was a domain takedown aimed at 10 domains, but because of how it was worded, around 84,000 innocent domains came down.

So there's a real need to identify what needs to be accomplished, the best way to accomplish it technically, and the best way to make sure that things are phrased properly so that they don't have these potential side effects. Thanks.

[Applause]

NII QUAYNOR: Thank you very much. I think we will move on to the last presentation, and that's going to be from Titi Akinsamni, from the University of Witwatersrand, South Africa.

TITI AKINSAMNI: Thank you, sir. This one? Yes. There we go. I'm so technology savvy.

Good evening, everyone. In the interest of having the graveyard shift -- it's been a very long day -- I'm going to run through my slides now and I will make a couple of comments at the end of it, so please bear with me.

I will speak slowly enough for the interpreters, but I will get through my slides a bit faster so that I can make a couple of points I have noted in our conversations.

So domain name takedowns, infringing Internet rights and freedom.

I am speaking as someone who is more often than not caught in between the process of understanding the reasons why domain name takedowns are important, sitting also in the seat of someone who believes firmly in the concept of "I have a right and I have a freedom to access, put up whatever it is that I need when I need to," and also sitting on the side of the fence where criminals have targeted me before, either that I am very crucial to some $3 billion that need to be moved from somewhere to somewhere or where they're claiming to be a long lost relative, or in some cases where actually my identity has been stolen and my credit card details have been used to do some awesome shopping. I wish I actually saw the products, but it's never happened so far.

So in presenting today, I'm going to speak to certain trends that I have seen. I will speak particularly to the case of South Africa.

Again, I'll mention I'm a Nigerian by birth. Yes! Do business with us! We are good people!

But I currently live in Johannesburg and I have for the last eight years.

And then I will speak particularly to the concept of moving us forward by respecting rights and freedoms, whatever approach that it is we choose to take.

And speaking particularly to the role that I see I can play.

George Orwell said in 1944 that the word "fascism" is almost entirely meaningless. Sometimes I agree with him, sometimes I don't. And that almost any English speaking person, I should say, would accept "bully" as a synonym for "fascist."

So Case 1. I'm not sure in this room how many people are aware of the ICE program. And particularly, I'm speaking to the takedown of rojadirecta.com.

I love soccer. I'm a (indiscernible) for life. Yes, I'm happy Manchester City beat Manchester United yesterday. But the issue is, sometimes because I live in a developing country, I don't have access to watch these matches, so I have to go to rojadirecta.com. Okay? And I visit the site and then one day I can visit it -- I can visit the forums, I can't access anything, and I realize, well, because I have enough information and because I have access to it, I have enough knowledge to be able to do it, I understand it's been taken down, even when clearly a case has been made by the Spanish courts that this site is legal. But another institution, another government, is able to take it down. Zip. That's it. Gone. Not just one, but also rojadirecta.org, okay? That's one case. I have titled that "No room for engagement. Take down. We ain't hearing nothing. You can bring the Pope, you can bring Dalai Lama, you can bring anybody. We're taking you down, we're taking you down, we're taking you down, finito."

All right. And then there's the WikiLeaks case. That I call it "takedown by stealth." "We warned you. Stop that content you're putting online."

And now I have to be very clear. This is in no way condoning, supporting, or being against what WikiLeaks does. That conversation is for a separate discussion.

This is about takedown.

So WikiLeaks is not taken down directly, but it's taken down by stealth.

I love James Bond. Some James Bond operations have been going on with WikiLeaks. So much so in the last 12 -- not even 12 hours. In the last 5 hours, the founder of WikiLeaks, Julian Assange, has had to announce that they have to stop publishing because they've run into financial trouble since someone somewhere -- Big Brother, I don't know who, no mention of any names, no institutions, government or private sector or otherwise -- have successfully blocked their ability to receive funding, even in the basic normal system.

That is a very, very interesting and very creative form of takedown.

Okay. Next slide.

So a case in point, South Africa, bringing it a bit closer to home. The Electronic Act in South Africa, it provides a protection for ISPs' liability, so when they do receive a notice to take something down and they act on it, they are protected, or where they do not act on it, then they're not protected and then I go "Ding, ding, ding."

So if you're the provider of the content, you are not necessarily covered. If you happen to be the one carrying that kind of content, the content being the domain name system right now, you are protected to a certain extent, but only if you follow what we say.

But somewhere sitting in the middle is going back to the conversation I had earlier about me needing to be able to watch my soccer and I can't afford to watch it in any other way.

What happens to the end user sitting in the middle?

As part of preparing for this session, I mentioned to Margie that I like legitimacy. I like having my facts right. And one of the things I needed to do was I went to the Internet Service Providers Association for South Africa and I requested certain data on the kind of takedowns they've received in the last year.

The first question I got was, "Who are you and why do you want that information?"

So very nicely I said, "Oh, I'm an Internet user and I think that's enough for me to be able to ask this question. It's not state material."

The next thing is, "No. Who are you and why do you want that information?"

Finally, I used the trump card. I said, "Oh, I'm an ALAC member of ICANN," and, boom, I got some information.

So it kind of works to be a member of ALAC, eh?

So I got information that since April 2005, there have been 284 takedown requests.

I have to slow down.

Now, what has occurred is with ISPA, the Internet Service Providers Association for South Africa, there are certain people -- there are certain members who have signed up such that if you have a takedown request, you're not going to have a problem with Go Daddy. It's clearly stated "This is the e-mail address you report each and every takedown request to, particularly."

Once you report it, though, there is no clarity in the owner of the actual domain name being informed.

So you could wake up this morning and be able to access the domain that you need, but in the next two minutes it's completely gone.

Now in 2010, there have been 148 takedown requests. Of that, about 80% have been honored. My next question to the provider -- to this membership organization was, Can I have the detail on the kinds of content -- the kind of domain names that have been asked to be taken down? I'm an optimist. I would ask. And I was told, No, we need some kind of formal recognition of who you are for us to be able to give you that information. It is not going to work. No more information given.

I am speaking too fast again. My apologies.

Long and short of it, I was shut down and I was told, You can't have that information. We'll need more information on who you are and what you want to use it for. So technically, if you do want to listen it for, this is what I needed it for.

Thank you. Next slide. So this is my suggestion. This is where I'm speaking from. And, again, I'm speaking to a room of informed people, so I'm very, very careful not to attempt to address the issues over and over again. The Internet has basic rights. Your human rights carry through all the way to your use of the Internet.

So this is what I believe that we need to be able to address, six of them. Internet access is for all. If it is for everybody, then you need to be able to ensure that if you are going to deny me access to some of the things that I need, that I am informed.

Second, freedom of expression and association. That is a long discussion. We won't go too much into it today. There is access to knowledge, shared learning and creation and a host of, I think, three more themes there. If you want more information on these particular rights, go to apc.org.

So I have spoken to the procedure in South Africa. This is the approach that I'm making a case for because I believe we were specifically told that we need to speak to what ICANN can do in some way.

One minute. Come on? How did it become one minute? I take back all the minute from all the other presenters from before. As the only woman technically speaking on this panel, I demand it. It is my right.

[Applause]

NII QUAYNOR: We heard you.

TITI AKINSAMNI: So the issue is raised. The first thing: Is it infringement? What kind of issue has been raised as abuse? And once an action needs to be preemptive, it needs to be made public. Till today we don't have a clear information from ICE on (indiscernible) and the Spanish courts legal -- We are not obeyed. That's what. The parties need to be informed.

Three is where conflict exists immediate rules need to be explored. Through each step, the Internet rights of all concerned must be taken into consideration.

Seeking answers, I am not purporting -- And my hands are raised up. Where I come from, it means "it is not me." But these are my suggestions, that if we were looking for some kind of system that would work for the three parties, meaning the law enforcement agencies, who have a right to be able to ensure we live online safely, to also ensuring the criminals are caught and that they are caught in time and that they are rightly removed when they need to be removed; to the third level where the end users, the individual users, the institutions, also are able to feel safe enough and feel that their rights have not been infringed. My question is: Who will bear the cost?

Second, what non-judicial but yet legal system can serve as a legal platform to resolve issues? I agree to a certain extent ICANN should not deal with content. But ICANN needs to be able to put itself in a place where domain name takedowns, particularly these issues, can be addressed. Exactly the fine details of how many hands make light work, I will say we need to put together some kind of institution, some kind of collective thinking that will address this.

And, of course, preventing negative influences. I gave two examples, one by stealth and the other by dictatorial, whatever you want to call it. By being a bully. That's the word for it.

We need to be able to find a system where it cannot be easily abused by political or private sector interests as well.

So in conclusion, I'd like to say this, that DNS takedowns is a complex maze. The industry governments that are able to follow through and address issues of DNS takedowns do it to some extent successfully. But the question mark remains that if I as an individual user needs to be able to report issues, where do I go to? That's a question that's not been answered.

And, of course, apart from recourse, there is recompense. If the gentleman who shot the Nigerian ambassador in Russia had some recourse, he would not have shot him. Thank you.

[Applause]

NII QUAYNOR: Thank you very much. I think we don't have too much time on our side. So I would like to go straight and get some comments from the floor, please.

DON BLUMENTHAL: If I could just mention real briefly, RojaDirecta is a prime example of how easy it is to get around some court orders. That's the kind of thing I was referring to. It was back up and accessible within a few minutes.

NII QUAYNOR: Please, go ahead, Bertrand.

BERTRAND DE LA CHAPELLE: Good afternoon. My name is Bertrand de La Chapelle. I'm currently on the ICANN board. And I used to be doing the previous four years the French GAC representative.

I want, first of all, to say how pleased I am to see the discussion deepening. I mean, in the course of the last one year and a half, be it here or at the IGF, the discussion on law enforcement challenges on DNS, in spite of all the problems that are currently emerging that I know, I see the discussion being multifactorial and it is good.

I want to raise two very quick points. The first thing is for Michael Moran. I appreciated the presentation very much. But if I look at the situation from an user perspective, in order to go to the Web site of the registrar to make a complaint, you need to basically understand the whole system and you've been exposed to something. Then you need to go to the WHOIS to see who was the guy who registered, what the registrar was, and so on.

So one of the questions I wanted to ask is what kind of discussions has there been towards other types of actors? I'm thinking, for instance, of resolvers or things that are what the users use to make it a simple reflexive, if you need to notify something. Maybe it is a stupid idea, and I would be happy to have the feedback.

The second point is related to what Titi was mentioning. I would like to formulate the problem she described about a director in ICE, for instance. As a very fundamental and legal and sovereignty problem, which is a question of jurisdiction, the problem we have today is the following question. How does a national government, A, feel when an activity by a citizen of that country, A, that is perfectly legal under the rules of that country are being prevented by the jurisdiction of country B simply because their domain name that this person is using has been bought through either a registrar in country B or ultimately, I suppose, even the registry of country B? In other words, can we formally say today that just because dot com and dot org are registries that are based in the jurisdiction of the United States, the United States jurisdiction legally is applicable to any activity conducted under a second-level domain registered under those registries? That's a very legal question.

NII QUAYNOR: Let's take something from the -- I think we should take a few. Please take this one.

MARGIE MILAM: I'm going to read a question from the chat. Anyone from the panel can answer it. The question is: How will DNS takedown work with peer-to-peer DNS that has no central control? Would anyone like to address that?

ROD RASMUSSEN: As the guy who has "technical" in his title, I guess I should take that one on. It depends, right? So, from the perspective of removing a domain from the root -- or from the TLD, it works the same. It doesn't matter whether it is peer-to-peer or not. Can you hear me? Okay.

From the perspective of filtering or blocking or things like that, it depends on where you're doing it.

Within your own network, again, it is not going to matter because your resolver -- your DNS resolver that you use, if that's the one that's doing the blocking or filtering, whatever resources you are protecting behind that will still work.

If the blocking or filtering is upstream, it is probably not going to work very well. So it depends on where you are doing the blocking, how you are doing the blocking. If you remove it entirely, it doesn't go away until caching kicks it. But it doesn't matter at that point, it is the same process.

NII QUAYNOR: Mike, I think you should jump in?

MICHAEL MORAN: I wanted to address Mr. de La Chapelle's question and observation. I thoroughly agree with you. I believe that we in law enforcement -- I say "us" first because we are letting the public down dreadfully in this area. Secondly, industry is letting them down terribly in this area.

I had an old sergeant years ago who used to say, "What would your mother think"? The reality is if my mother tried to report losing money on eBay or something like that, I say online, she can't do it. It is not -- It is because we are still last in the fog of it.

So you talk about a browser. The biggest problem we have in this area, we all have, law enforcement, industry, academia, civil rights people, everybody has, is metrics. Nobody knows how big this problem is. Nobody knows what the definition of this problem is. So in one country, cybercrime is defined differently than in another. And reports of cybercrime are taken in different ways in different countries, if at all.

And the result is we cannot have proper policy. We cannot tackle difficult issues like Titi spoke about without actually knowing the scale of it. And that for me -- so, yep, browser button, a reporting platform, absolutely.

NII QUAYNOR: Thank you. I will take two questions and then I will have them respond.

Alex?

ALEJANDRO PISANTY: Good afternoon. My name is Alejandro Pisanty. I'm a professor at the National University of Mexico and chair of the Internet society in Mexico as well. Domain name blocking, filtering, et cetera, shares a lot of characteristics with all forms of blocking on the Internet which was built to go around blocking.

To illustrate this problem, I want to express my personal great respect for Mick Moran and tell him I have not been able to communicate with him because INTERPOL is blocking my University e-mail. I have to come from Mexico to Dakar. That's about 9600 kilometers -- the way actually requires about 18,000 kilometers of lights through European capital airports -- to tell him I do like him very much, and I respect his work very much and a few more things, which are the following.

The problems with blocking that we are seeing are fundamental. It's necessary to solve. The human conduct problem that we face which is called crime, fraud, child abuse, there are huge enormous consequences and ramifications.

In the IGF session of Kenya last month or early this month, there was an extraordinary example to illustrate where we have to focus our efforts, which was an Australian law enforcement official describing the tracing of heinous crimes, particularly among them someone selling live sex with minors over the Internet. To illustrate where we have to go with this, this man was the two girls' father.

We are not going to fix that problem by blocking, filtering and continuing to create more and more elaborate ways to authenticate, authorize, deny, block, ban. We have to continue to focus as human beings, as members of society, in the buildup and the loss of institutions and on the psychology and sociology of humans who commit crimes.

We have to create tools that serve to compensate the effects of this free flow of information when it is for evil purposes.

But the focus is the conduct and the ways to implement all the traditional institutions. This is a Layer 8 problem. We need more Layer 8 tools. Once we have those Layer 8 tools, once we have freedom of speech, once we have rights on the Layer 8, on the institutional level, then we can go back down into them.

A forum like ICANN, a forum like the Internet Governance Forum and specialized forums like the APWG and so forth, those multistakeholder mechanisms are the place we have to meet. And we have to, of course, less of this bouncing, like you do what I want. You are damaging what I want when I do what you want and be more like after what are the roles we share. Thanks.

WENDY SELTZER: Thank you. Wendy Seltzer, councilor from the noncommercial users constituency and in this context relevant perhaps also founder of the Web site chillingeffects.org which reports on legal threats and helps users to understand why often Web sites and other online content is unavailable because complaints have been made against it.

And so as we're thinking about tools for takedowns and making takedowns more rapid, Rod address this particularly to you because you were presenting a tool which sounds useful to take some of the static out of conversations. Are you thinking about transparency and how users of the Internet and researchers like Titi can find out why names have been no longer resolved, what has happened to their content, and what users might be able to do for redress if there was, in fact, some legitimate content associated but it was used for e-mail and so wasn't visible in a Web search?

What can we do to improve the transparency of takedown to help the public ensure that it's used in only legitimate cases?

NII QUAYNOR: Any comments from the panel?

ROD RASMUSSEN: I'll address the last one since it was directed straight at me. And, Wendy, that's exactly what we're trying to do with this system, is actually increase the amount of -- the ability for people to see what's going on because right now we have a very unaccountable system where everything is done on an ad-hoc basis between people who know each other or people who are receiving reports and doing things based on those reports. The idea behind this APWG system is that there would be statistics published about content removals, what was requested, all those kinds of things. We work with lots of research partners, academia, so they can share that data with them so they can get studies out on that and elaborate on various other issues.

There is also a redress mechanism built into the system as well so there can be immediate feedback based on people taking action.

So those are certainly concerns that we wanted to address in building the system. We've heard a lot from folks like yourselves over the years about these various concerns, and we share them as well. We do not want to take down legitimate content out there, even controversial content. This is all about going after the things that we pretty much agree are problems for the entire Internet, which is phishing and malware operations.

NII QUAYNOR: Okay. I think what we'll do is we'll take the comments and questions you have, and then they will respond in their closing statements. No more joining of queues. We just want to hear you, and then we'll try and respond to the comments you have.

So, please, Mouhamet.

MOUHAMET DIOP: Thank you, Chairman. I just want to when you look at the number of actors working in the area of (indiscernible) and law enforcement for the DNS, I want to separate two cases: The case for the ccTLDs and the case for the gTLDs. It is very important for me.

And on the other side, I want to put in front two main actors in terms of intervention and action. The regulations and the law in terms of global actors inside, you will find police, court, whatever you want.

Here is a case. If you look at example of the mobile sector because a lot of money are going there, the regulation have put a lot of infrastructure interfacing in order to sort out problems. And I'm pleased to announce that one of the best resolution environments that I have seen for the mobile market is in Nigeria.

They create a court for the mobile industry, where every three months, it is chaired by the regulator. All the mobile actors come and they see files and complaints. And they get a (indiscernible) each region and people have a way to complain and the instances are sought out. And they come back in the last two months to see what was done and if there are any results.

Let's come back on the domain name business. What's happening here is I'm a registry in Senegal. When people get a problem, the first thing they don't know who to talk to. The regulations in our environment, I'm sorry to say that they have no clue regarding the problem of the Internet business. They are not concerned. There is no money flowing. They don't learn about it so there is a capacity-building issue. They need to be trained at least to ask to the relevant organization to deal with problem.

If I got a problem of cybercrime, I'm telling you, you can go through a process of months and months, years and years, even you will have a police agent in front of you. The first thing he will spend months and months to understand what you are talking about. I'm serious.

If it is a ccTLD problem, you might be lucky that at the end of the day, they will direct you to the ccTLD who will have nothing in front in order to sort out the problem but at least can listen to you and recognize that it is a case of abuse and that's it because the court in itself, the law in the countries are not to deal with the cybercrime. There was no mechanism, no interface that the registrant, that the user can come and talk.

So my suggestion to ICANN and to the organization and to the players is we need to have a structured way of enforcing and supporting through best practice. Countries need to have guidance on how to deal with problems. Some of them are related to the law. Some of them are related to the regulation in terms of organizing the market, organizing the actors, organizing all these different institutions that intervene in the sector in order to get guidance.

I'm telling you if you don't sort it out, the African registrant or the third-world registrant will have no confidence in the system and they will not put their basket in it. At the end of the day, don't be surprised to see a very low level of introduction of domain names in the country because people say, What's going to happen if I get a problem with my reseller or my integrator or my Web hoster? If he don't find an answer to these questions, he say, "I prefer to be in real face-to-face, physical transaction life rather than going into virtual." Thank you.

NII QUAYNOR: Thank you.

>> I guess part of my question he already asked. I'm going to -- the takedowns with Ms. Titi. I mean, there is a lot of takedowns. There is a lot of questions asked about that. Now, you take down a Web site. The I.P. address is still there. They change the name and then come back with the same concept, with the same thing. When it comes to downloading films, it is the same thing going on. So why can't you go back the I.P. address and then just delete it from the site -- I mean, from the worldwide Web?

(Speaker off microphone).

>> Please answer me in name and terms so I can understand because I'm not that technical.

And the scams are coming to Africa like tsunami. I mean, all the bad stuff are coming here. The Nigerian nightmare is (indiscernible) don't even worry about it. So what can you guys do about the legislations and laws and stuff like that? I guess that's his question. Thank you.

NII QUAYNOR: Yes, ma'am?

RAFIDAH MAT ISA: Hi. My name is Rafidah. I'm from the Malaysian Communications and Multimedia Commission. I have a question for Rod actually.

The tools that you have -- because at the moment, our commission, we handle blocking, so sorry to say. But we are more concentrate on the phishing blocking because it is for the people -- because we don't want people to get cheated by the Web sites.

So at the moment, we had a very good relationship with a lot of service providers like Google or Yahoo!. And whenever we contact them, they can stop the Web site in just about a few minutes. We send them now, they close the Web site in one or two minutes.

So the problem that we have is certain Web sites that are not hosted by these big companies, they are -- sometimes there is no response at all. So we use another way which is we block the DNS. So using your new tools is quite good. So definitely I'm going back to try it.

Just want to know, how long is -- how fast is the response time? Because at the moment, we have two hours for the service providers to block any phishing Web site. But if your Web site can -- if you are hosting, it can be faster. So we can try that. Thank you.

NII QUAYNOR: Last comment.

HAMZA ABOULFETH: Yes. Hi, I'm Hamza Aboulfeth from Morocco, browser Web host and ICANN accredited registrar. The question is a direct question obviously. And I would like to know as a Moroccan company what laws we should apply and comply to. Are these Moroccan laws, U.S. laws or Canadian laws as we have our servers located in Canada? And as we can have them, like, in France or something.

Does this depend on the location -- our location, or can some day a policeman from Morocco just come and just knock at our office door -- and that happened -- and ask for some information to take down a Web site or stuff like that.

And, also, I will join Mouhamet on what he said about being in Africa and this thing to have our end users understand the meaning of how to contact in case of a problem if you actually buy a Web site from some guy that he will just disappear from one day to another and you will just be left with nothing, with no domain name, with no Web site or anything.

So who should we turn to get this problem fixed once and for all?

NII QUAYNOR: Well, thank you very much. At least we've got some very good questions. And what we'll do, we'll start from my extreme right and ask my panelists to make their closing comments. So, please, Titi. Short time.

TITI AKINSAMNI: I really wish I could do short-term. I will try. I just went to the online -- I went to the Webcast of our session, and I realized a comment has been made there. It is public, so I can say it. (Indiscernible) has indicated that somehow it has been clichés that has come through. And I was going to respond and this is how I'm going to do my closing remarks. We cannot run away from clichés and repeating issues as long as they have not been addressed.

A typical example is one of the questions that's come through here, why don't you just take down the I.P. address. (Gasping.) Why?

As long as the issues are not fully understand and fully addressed and we assume that everybody fully gets it, we are not going to move anywhere.

My second comment is this: In terms of DNS takedown, we move forward, yes. But also the proposals we have in front of us, what are we going to do with? When are we going to move beyond the speeches and panels like this and actually take action on it? I presented a couple of ideas. Whatever it is we need to do, I think, needs to be done ASAP, otherwise we keep getting this continuous who is right, LEAs, governments or individual user, other providers who are providing content that people say no to. Thank you.

NII QUAYNOR: Yes?

DON BLUMENTHAL: I would like to address the last two comments from that side of the room. First, what laws you have to pay attention to or think about is still an evolving field. I mean, right off the top, if you got servers in Canada, you need to pay attention to Canadian law. If you are based in Morocco, you need to pay attention to Moroccan law.

The gray areas are, for example, what ICE did with respect to rojadirecta, and that is being litigated on a few different levels.

With respect to bringing down an IP number, let's just back up. We're talking about domain takedowns, which is a very different issue, but, again I'll used our favorite case here, rojadirecta. Let's assume we can pull the IP number for rojadirecta.org. That content is also on rojadirecta.es, and I believe it was on rojadirecta.se.

So an IP-based approach just is not -- is not any magic bullet. It's hosted in multiple places. It can be copied around. There are alternate methods to get to it.

ROD RASMUSSEN: Just for reference on that, see the Fast Flux working group work.

DON BLUMENTHAL: Right.

ROD RASMUSSEN: Did you have any more comments, Don? Okay. To address the --

NII QUAYNOR: As brief as you can.

ROD RASMUSSEN: I will be very brief.

To address the MyCERT question, the APWG program is a suspension program. It gets the domain removed completely from -- you know, so nobody on the Internet can see it.

If you're doing things in two hours, stick with it. That's about as good as you're going to get it done.

With the Registry Suspension Project, that's going to take probably -- when we're up and running, hopefully less than a day, but it's a suspension project. It's not -- it's far more serious, I think, than blocking a certain portion of the Internet from seeing content.

That was my only comment because the other stuff has been covered. Thanks.

NII QUAYNOR: If you don't have a comment, you don't have to make one.

MICHAEL MORAN: Certainly. I've just agreed with Fred that we'll make one comment between us, which is really addressing the raising capability of law enforcement, not just locally here for the registrar but globally.

We're doing a lot of work in this effort, in this particular area as law enforcement, because the threat is global and we need to outreach to as many countries as possible, so please be reassured that that work is being undertaken. It's a slow process and obviously the work that Fred had spoken about within the region will slowly bear fruit. Thank you.

LANRE AJAYI: Oh, okay. Nigeria (indiscernible) fighting cybercrime today because of three major reasons. One, we admitted there was a problem and we were determined to fight it.

Two, we did extensive international collaboration. That has been confirmed on this panel.

And collaboration is the only way to deal with cybercrime, especially when it's in (indiscernible) jurisdiction. Some other (indiscernible) jurisdiction. You can only fight cybercrime (indiscernible) jurisdiction (indiscernible) collaboration. We do that extensively, and we are extremely happy in bringing down the cybercrime rate.

And we also adopted the multistakeholder engagement. That's what Mohamet was referring to. (indiscernible) we try to put together to discuss it and get them involved in fighting cybercrime, and the result is that cybercrime is going down in Nigeria.

Thank you.

PIERRE DANDJINOU: Thank you. Briefly, I think he said it, collaboration, but I would also like to add the whole issue about capacity development and especially when it comes to Africa, I do believe that we need to continue.

And then specific countries also need their own sort of cyber security strategy. Sometimes people are very -- don't know what to do inside countries. And finally, the best practices that we need to spread and I think Africa cert is out for that.

NII QUAYNOR: Thank you. Okay. I think you've done a good job for staying with us. It's been a long show, but I think Bertrand is right, the discussion is deepening and I'm glad that some of it is happening on the continent here. So with that, I thank you very much for your participation.

[Applause]